The 2-generator restricted Burnside group of exponent 7

E.A. O'Brien and Michael Vaughan-Lee

Abstract

We report on our construction of a power-commutator presentation for $R(2,7)$, the largest finite 2-generator group of exponent 7. Our calculations show that $R(2,7)$ has order 7^{20416}, nilpotency class 28, and derived length 5. The calculations also imply that the associated Lie ring of $R(2,7)$ satisfies relations which are not consequences of the multilinear identities which hold in the associated Lie rings of groups of exponent 7.

1 Introduction

We have constructed a consistent power-commutator presentation for $R(2,7)$, the largest finite 2-generator group of exponent 7. We can read off from the presentation that $R(2,7)$ has order 7^{20416} and nilpotency class 28. An easy calculation with the power-commutator presentation shows that $R(2,7)$ has derived length 5. It also may be of interest that $R(2,7)$ satisfies the 10-Engel identity, but not the 9-Engel identity.

Newman & Vaughan-Lee [10] constructed presentations for two Lie algebras connected with $R(2,7)$. First they constructed $E(2,7)$, the free 2-generator 6-Engel Lie algebra over $\mathbb{Z}_7$, and showed that it has class 29 and dimension 23789. The associated Lie rings of groups of exponent 7 satisfy the 6-Engel identity $[x,y,y,y,y,y,y]=0$, and since they have characteristic 7 they may be viewed as Lie algebras over the field $\mathbb{Z}_7$. Thus if $L(2,7)$ is the associated Lie ring of $R(2,7)$, then $L(2,7)$ is a homomorphic image of $E(2,7)$.

However, $L(2,7)$ is known to satisfy identities which are not consequences of the 6-Engel identity. (This was first discovered by Khukhro [6].) More generally, the associated Lie rings of groups of exponent p satisfy a sequence of multilinear identities $K_n=0$ for $n \geq p$. See Theorem 2.4.7 and Theorem 2.5.1 of [13] for

This work was supported in part by the Marsden Fund of New Zealand via grant #9144/3368248. 2000 *Mathematics Subject Classification.* Primary 20D15.

a description of these identities. By Theorem 2.5.1 of [13], all the multilinear identities which hold in the associated Lie rings of groups of exponent 7 are consequences of these identities.

The $(p-1)$-Engel identity is equivalent in characteristic p to the identity $K_p = 0$. Let $W(m,p)$ denote the largest m-generator Lie algebra over $\mathbb{Z}_p$ satisfying the identities $K_n = 0$ for $n \geq p$. So $L(m,p)$, the associated Lie ring of $R(m,p)$, is a homomorphic image of $W(m,p)$. Newman & Vaughan-Lee [10] also constructed $W(2,7)$, and showed that it has class 29 and dimension 20418. Since our computations show that $R(2,7)$ has class 28, it follows that $L(2,7)$ is a *proper* homomorphic image of $W(2,7)$. In fact $L(2,7)$ is the class 28 quotient of $W(2,7)$: namely,

$$L(2,7) \cong W(2,7)/W(2,7)^{29}.$$

Thus the associated Lie ring of $R(2,7)$ satisfies relations which are not consequences of the multilinear identities $K_n = 0$. This is in contrast to groups of exponent 5. Havas, Wall & Wamsley [4] showed that

$$L(2,5) \cong E(2,5) \cong W(2,5),$$

and it was proved in [12] that

$$L(3,5) \cong W(3,5).$$

Groups of exponent 2 are elementary abelian, and groups of exponent 3 are nilpotent of class at most 3. It is easy to see that

$$L(m,p) \cong E(m,p) \cong W(m,p)$$

for $p = 2,3$ and for all m.

We constructed the power-commutator presentation for $R(2,7)$ using a special-purpose implementation of the p-quotient algorithm. We made a number of modifications to the general-purpose algorithm described in Newman & O'Brien [9] to enable us to carry out this computation. In particular, we used a modified data structure to save space, used automorphisms and commutator identities to facilitate enforcing the exponent law, and used the Baker-Campbell-Hausdorff formula to compute part of the power-commutator presentation. Our modified data structure is that used by Newman & Vaughan-Lee [10]. Automorphisms and commutator identities were used in the study of Burnside groups by Newman & O'Brien [9] and Vaughan-Lee [12]. We believe that this use of the Baker-Campbell-Hausdorff formula is new, and estimate that its use reduced the time required for the construction by a factor of at least 8.

All CPU times reported in the paper were obtained on a Sun UltraSPARC Enterprise 4000 server, having 3 GB of RAM. The construction and verification of the power-commutator presentation for $R(2,7)$ took approximately 7725 CPU hours and used a maximum of 1.5 GB of RAM. (For calculations of this sort it is important to have the whole presentation in RAM.)

The paper is organised as follows. In Section 2 we review basic features of the p-quotient algorithm. In Section 3 we discuss the modified data structure. In Section 4 we discuss enforcement of the exponent law, and in Section 5 we discuss the use of the Baker-Campbell-Hausdorff formula. We report on the resources used in Section 6 and finally comment on the accuracy of our computation.

We are particularly grateful to M.F. Newman for a number of useful discussions on how to construct $R(2,7)$. Our approach also draws heavily on the work of Newman & Vaughan-Lee [10] on Lie algebras associated with $R(2,7)$.

2 The p-quotient algorithm

If G is a group of order p^n where p is a prime, then G can be described using a *power-commutator presentation.* This is a presentation on a generating set $\{a_1, a_2, \ldots, a_n\}$ with n power relations

$$a_i^p = a_{i+1}^{\alpha(i,i+1)} a_{i+2}^{\alpha(i,i+2)} \ldots a_n^{\alpha(i,n)}, \tag{1}$$

where $0 \leq \alpha(i,k) < p$ for $1 \leq i < k \leq n$, and $\binom{n}{2}$ commutator relations

$$[a_i, a_j] = a_{i+1}^{\alpha(i,j,i+1)} a_{i+2}^{\alpha(i,j,i+2)} \ldots a_n^{\alpha(i,j,n)}, \tag{2}$$

where $0 \leq \alpha(i,j,k) < p$ for $1 \leq j < i < k \leq n$. These presentations are of central importance in allowing effective computation with finite p-groups (see Sims [11]). However, a group defined by a power-commutator presentation on n generators may have order dividing p^n.

A critical feature of a power-commutator presentation is that every element of the presented group may be written as a *normal word* $a_1^{\alpha_1} a_2^{\alpha_2} \ldots a_n^{\alpha_n}$ where each α_i is an integer and $0 \leq \alpha_i < p$. An arbitrary word in the generators is converted to an equivalent normal word by a process called *collection.* Various strategies for collection exist; a general discussion can be found in [11, §9.4]. If every element has a unique normal form, then the power-commutator presentation is *consistent* (and so defines a group of order p^n). Collection using a consistent presentation provides a solution to the word problem. The standard method to construct a consistent power-commutator presentation from an inconsistent one is described in Appendix B of [13].

The general-purpose implementation of the p-quotient algorithm is used to construct consistent power-commutator presentations for finite p-groups, described by a finite presentation or an exponent law. The algorithm in common use today is based on the "Canberra nilpotent quotient algorithm" originally developed by Havas & Newman [3]. Over the years this algorithm has been improved and extended in a number of ways. For a description of the general-purpose algorithm and a report of some of these improvements, see Newman & O'Brien [9]. For further details see Newman, Nickel & Niemeyer [8]. Here we focus on its application to groups of *exponent* p, and so some details are simplified.

The algorithm works along the lower central series of G: having computed a consistent power-commutator presentation for the largest class $c-1$ quotient, $G/\gamma_c(G)$, of G it computes one for the largest class c quotient, $G/\gamma_{c+1}(G)$.

In practice, the consistent power-commutator presentations constructed by the p-quotient algorithm have additional structure.

1. If $G/\Phi(G)$ has rank d, then $\{a_1, \ldots, a_d\}$ is a generating set for G.

2. For each a_k in $\{a_{d+1}, \ldots, a_n\}$, there is at least one relation whose right hand side is a_k. One of these relations is taken as the *definition* of a_k.

3. The power-commutator presentation also has an associated *weight* function: a generator a_i is assigned a weight $\omega(a_i)$ corresponding to the class at which it is added. The value of ω on the generators is the following.

   (i) $\omega(a_i) = 1$ for $i = 1, \ldots, d$;

   (ii) if the definition of a_k is $a_i^p = a_k$, then $\omega(a_k) = \omega(a_i) + 1$;

   (iii) if the definition of a_k is $[a_j, a_i] = a_k$, then $\omega(a_k) = \omega(a_j) + \omega(a_i)$.

   Note that $\omega(a_n)$ is the class of G. This weight function is extended to all normal words in a natural way: if a generator a_i has weight $\omega(a_i)$ for $i = 1, 2, \ldots, n$, then $a_1^{\alpha_1} a_2^{\alpha_2} \ldots a_n^{\alpha_n}$ has weight $\sum_{i=1}^{n} \alpha_i \omega(g_i)$.

The implementation of the general-purpose algorithm by Newman & O'Brien [9] is available both as a stand-alone program, and as a component of GAP and Magma. In principle, it can be used to compute a power-commutator presentation for $R(m, q)$ for an arbitrary number of generators m and an arbitrary prime-power exponent q. Our investigations suggest however that it would take thousands of CPU years and several GB of RAM to construct a presentation for $R(2, 7)$ using this implementation. Hence we made a number of modifications to the algorithm to save both time and space. As previously mentioned, our resulting implementation constructed the presentation in approximately 7725 CPU hours and used a maximum of 1.5 GB of RAM.

3 The data structure

An implementation of the p-quotient algorithm must store the p-th powers and the commutators of the power-commutator presentation generators. In practice, the program must know the coefficients $\alpha_{(i,j)}$ $(1 \leq i < j \leq n)$ and $\alpha_{(i,j,k)}$ $(1 \leq j < i < k \leq n)$ from equations (1) and (2). There are $(n^3 - n)/6$ such coefficients.

Recall that a consistent power-commutator presentation for $R(2,7)$ has 20416 generators. This suggests that we might need to store $1,418,275,888,480$ coefficients. Fortunately, most of these coefficients are zero and we exploit this. Recall that a generator has weight w if it lies in $\gamma_w(G)\backslash\gamma_{w+1}(G)$. Consider two generators a_i, a_j of weights u, v respectively. Since $[\gamma_u(G), \gamma_v(G)] \leq \gamma_{u+v}(G)$, the commutator $[a_i, a_j]$ only involves generators of weight at least $u+v$. In other words, $\alpha_{(i,j,k)} = 0$ unless a_k has weight at least $u+v$. In particular $[a_i, a_j]$ is trivial if $u+v$ is greater than the nilpotency class of G. The saving that this represents depends on the distribution of weights among the generators of G. In the case of $R(2,7)$ there remain $1,950,874,630$ coefficients $\alpha_{(i,j,k)}$ which could be non-zero; if each was stored as a single 32-bit integer, then we would need almost 8 GB to store a power-commutator presentation for $R(2,7)$. In practice, a large proportion of these remaining coefficients are zero, although generally it is not possible to predict which ones. The implementation of the general-purpose p-quotient algorithm only stores the commutator $[a_i, a_j]$ if weight considerations imply that it may be non-trivial. In such cases, its value is stored as a sequence of *generator-exponent* pairs: if

$$[a_i, a_j] = a_r^\alpha a_s^\beta \ldots a_t^\gamma$$

where $r < s < \ldots < t$ and $\alpha, \beta, \ldots, \gamma$ are non-zero exponents, then the value of $[a_i, a_j]$ is stored as the sequence

$$(r, \alpha), (s, \beta), \ldots, (t, \gamma),$$

where each generator-exponent pair is stored as a single 32-bit integer. Using this technique, the power-commutator presentation for $R(2,7)$ could be stored in just over 2 GB.

However, much larger power-commutator presentations are generated at intermediate stages in the calculation. Hence we adopted a different strategy to store commutators. For each non-trivial commutator $[a_i, a_j]$, we treated the coefficients $\alpha_{(i,j,k)}$ $(i < k \leq n)$ as a vector of length $n - i$. We noted the positions of the first and last non-zero entries in this vector, and stored the coefficients between these two positions as a sequence of 32-bit integers, packing 10 coefficients into each integer. Since the coefficients lie in the range 0 to 6, only 3 bits are needed to store a single coefficient. This strategy enabled us to store the power-commutator presentation for $R(2,7)$ in 660 MB and to complete the calculation in a maximum of 1.5 GB of RAM. This space saving strategy was also employed in [10].

4 Exponent checking

We now consider the construction of a power-commutator presentation for $R(2,7)$ in some more detail. Initially, the p-quotient algorithm constructs a power-commutator presentation for the largest abelian quotient of $R(2,7)$. Suppose that the class c quotient of $R(2,7)$ is G. The general-purpose algorithm first constructs a power-commutator presentation for the 7-*covering group* of G – this is the largest group H with an elementary abelian central subgroup M contained in the Frattini subgroup $\Phi(H)$, with $H/M \cong G$. The subgroup M is the *p-multiplicator* of G and the class $c+1$ quotient of $R(2,7)$ is H/H^7. The algorithm now determines a generating set for H^7 by evaluating h^7 for certain elements $h \in H$. If, for example, H is the 7-covering group of the class 27 quotient of $R(2,7)$, then H has order 7^{39495}. Further $H/H^7 \cong R(2,7)$ which has order 7^{20416}. Hence H^7 is elementary abelian of rank 19079 and so computing a generating set for H^7 by this method would involve computing h^7 for at least 19079 elements h. In practice, the general-purpose algorithm would need to evaluate many more 7-th powers. The standard method of computing h^7 is to write h as a normal word, concatenate 7 copies of this word, and then apply the collection process to obtain the normal word for h^7.

In our computation of the class 28 quotient of $R(2,7)$, the collection of $(a_1a_2)^7$ took approximately 12 CPU days. Hence it would be impossible to evaluate many thousands of 7-th powers by collection. We now outline how we modified the general-purpose p-quotient algorithm so that we only needed to compute just *one* 7-th power in this way: namely, $(a_1a_2)^7$.

Let G be the class c quotient of $R(2,7)$, and suppose that G has order 7^n, and power-commutator presentation generators $a_1, a_2, \ldots, a_n$. Let H be the 7-covering group for G. The power-commutator presentation generators of H are of two types. First, H has n generators corresponding to the power-commutator presentation generators of G, and these are usually also denoted $a_1, a_2, \ldots, a_n$. Then H has additional power-commutator presentation generators $a_{n+1}, a_{n+2}, \ldots, a_t$ corresponding to the generators of the p-multiplicator M. Every element of H can be uniquely expressed as a normal word

$$a_1^{\alpha_1} a_2^{\alpha_2} \ldots a_t^{\alpha_t}$$

with $0 \leq \alpha_i < 7$ for $i = 1, 2, \ldots, t$. Now the elements of M are central in H and of order 7, so

$$\left(a_1^{\alpha_1} a_2^{\alpha_2} \ldots a_n^{\alpha_n} a_{n+1}^{\alpha_{n+1}} \ldots a_t^{\alpha_t}\right)^7 = \left(a_1^{\alpha_1} a_2^{\alpha_2} \ldots a_n^{\alpha_n}\right)^7 .$$

Recall G has exponent 7; hence if $h \in H$, then $h^7 \in M$, and so h^7 is central in H. Thus, if $h, k \in H$ and hM is conjugate to kM, then $h^7 = k^7$. We choose a set of representatives for the conjugacy classes of non-trivial cyclic subgroups of G, and we choose a set S of normal words in $a_1, a_2, \ldots, a_n$ such that $\{sM \mid s \in S\}$ contains a generator for each representative subgroup. Then H^7 is generated by $\{s^7 \mid s \in S\}$.

The structure of S is of some importance. We construct S using the Felsch & Neubüser algorithm [2] for computing conjugacy classes of p-groups. This algorithm proceeds as follows. For each k with $1 \leq k \leq n+1$ we let G_k be the subgroup of G generated by $\{a_k, a_{k+1}, \ldots, a_n\}$. It is important to note that the generators a_i for $i = 3, 4, \ldots, n$ have definitions. We assume that $a_3 = [a_2, a_1]$, $a_4 = [a_2, a_1, a_1]$, $a_5 = [a_2, a_1, a_2]$, and that the weights of the a_i form a non-decreasing sequence. First we choose a set of representatives for the conjugacy classes of G/G_3. Since G is generated by a_1 and a_2,

$$\{a_1^\alpha a_2^\beta \mid 0 \le \alpha, \beta \le 6\}$$

is such a set. We extend this set to a set of representatives for the conjugacy classes of G/G_4. If α, β are not both zero, then $a_1^\alpha a_2^\beta$ is conjugate to $a_1^\alpha a_2^\beta a_3^\gamma$ modulo G_4 for all γ, and so

$$\{a_1^\alpha a_2^\beta \mid 0 \le \alpha, \beta \le 6\} \cup \{a_3^\alpha \mid 1 \le \alpha \le 6\}$$

is a set of representatives for the conjugacy classes of G/G_4. We now extend this set to a set of representatives for the conjugacy classes of G/G_5, and so on.

Suppose we have a set S_k of representatives for the conjugacy classes of G/G_k of the form $a_1^{\alpha_1} a_2^{\alpha_2} \ldots a_{k-1}^{\alpha_{k-1}}$. We obtain a set S_{k+1} of representatives for the conjugacy classes of G/G_{k+1} as follows. Every element of G is conjugate modulo G_{k+1} to an element $s a_k^{\alpha_k}$ for some $s \in S_k$. If $s \in S_k$ and s is conjugate to $s a_k$ modulo G_{k+1}, then s is conjugate to $s a_k^{\alpha_k}$ modulo G_{k+1} for all α_k. Hence we define $S_{k+1} = T \cup T'$ where

$$T = \{s \in S_k \mid s \text{ is conjugate to } s a_k \text{ modulo } G_{k+1}\},$$

and

$$T' = \{s a_k^{\alpha_k} \mid s \in S_k,\ 0 \le \alpha_k \le 6,\ s \text{ is not conjugate to } s a_k \text{ modulo } G_{k+1}\}.$$

Iterating, we obtain a set S_{n+1} of representatives for the conjugacy classes of G. The elements of S_{n+1} are normal words of the form $a_1^{\alpha_1} a_2^{\alpha_2} \ldots a_n^{\alpha_n}$, and we take our set S of generators for representatives of the conjugacy classes of non-trivial cyclic subgroups of G to be the non-trivial elements $a_1^{\alpha_1} a_2^{\alpha_2} \ldots a_n^{\alpha_n}$ of S_{n+1} with the property that the first non-zero entry in the sequence $(\alpha_1, \alpha_2, \ldots, \alpha_n)$ is 1.

The set S constructed in this way has two key properties: if $a_1^{\alpha_1} a_2^{\alpha_2} \ldots a_n^{\alpha_n} \in S$, then $a_1^{\alpha_1} a_2^{\alpha_2} \ldots a_k^{\alpha_k} \in S$ for all non-trivial initial segments $a_1^{\alpha_1} a_2^{\alpha_2} \ldots a_k^{\alpha_k}$ $(1 \le k \le n)$; also if $a_1^{\alpha_1} a_2^{\alpha_2} \ldots a_n^{\alpha_n} \in S$ and either α_1 or α_2 is non-zero, then $\alpha_3 = 0$. Hence S contains words of three types:

1. power-commutator presentation generators a_r;
2. the words $a_1 a_2^i$ $(1 \le i \le 6)$;
3. normal words of the form $a_r a_s^\alpha \ldots a_t^\beta$ where $\beta \ne 0$, and a_t has weight at least 3.

We used different methods to ensure that words of each type have order 7.

Our implementation of the p-quotient algorithm stores the p-th powers of the power-commutator presentation generators, so it is easy to verify that a generator has order 7 by checking that the stored value is trivial. In practice, we modified the general-purpose algorithm so that the 7-th powers of generators are trivial throughout the calculation.

We computed $(a_1a_2)^7$ by applying a collection process to the word

$$a_1a_2a_1a_2a_1a_2a_1a_2a_1a_2a_1a_2a_1a_2$$

in the standard way. This collection gave us an element m of the p-multiplicator M. We then computed the images of m under powers of the automorphism mapping a_1 to a_1a_2 and mapping a_2 to a_2. This gave the values of $(a_1a_2^i)^7$ for $i = 2, 3, 4, 5, 6$. At class 28, it took about 12 CPU days to compute the value of m, but "only" about 2.7 days to compute the images of m under powers of this automorphism.

We decomposed normal words of the form $a_r a_s^\alpha \dots a_t^\beta$ where a_t has weight at least 3 as words $u.v^\beta$, with $v = a_t$. Since v is a generator of weight at least 3, it follows that the group generated by u and v is a proper homomorphic image of $R(2,7)$. Below, we deduce some commutator identities $q_i(u,v) = 1$ $(i = 1, 2, \dots, 6)$ satisfied by u, v, and prove that evaluating these identities is equivalent to evaluating $(u.v^\beta)^7$.

These identities were obtained as follows. If we consider a commutator w in u, v, where there are b occurrences of u and c occurrences of v in w, then using the fact that v has weight at least 3 we deduce that the weight of w is at least $b + 3c$. The Lie algebra calculations showed that $R(2,7)$ has class at most 29 (although the actual class turned out to be 28), and so w must be trivial if $b + 3c > 29$.

We first constructed the largest group K of exponent 7 satisfying the following properties:

(1). K is generated by two elements u, v;

(2). if w is any commutator of weight b in u and weight c in v where $b + 3c > 29$, then $w = 1$.

(This is an easy computation using the general-purpose p-quotient algorithm.)

We next observe that each of the following six products of commutators of weight 7 is an element of $\gamma_8(K)$.

$$\begin{aligned}
&[v,u,u,u,u,u,u],\\
&[v,u,u,u,u,u,v]^3[v,u,u,u,u,v,u]^4[v,u,u,u,v,u,u],\\
&[v,u,u,u,u,v,v]^4[v,u,u,u,v,u,v][v,u,u,u,v,v,u]^6[v,u,u,v,u,v,u]^4[v,u,u,v,v,u,u],\\
&[v,u,u,u,v,v,v]^3[v,u,u,v,u,v,v]^2[v,u,u,v,v,u,v]^4[v,u,u,v,v,v,u]^5[v,u,v,v,u,v,u],\\
&[v,u,u,v,v,v,v][v,u,v,v,u,v,v]^3[v,u,v,v,v,v,u],\\
&[v,u,v,v,v,v,v].
\end{aligned}$$

We obtained the identities $q_i(u,v)=1$ $(i=1,2,\ldots,6)$ by expressing each element as a product of commutators of weight 8 or more in u and v (and so we deduce six relations for K). It is relevant for our use of these identities to note that all of the commutators occurring in the expression for $q_i(u,v)$ have weight at least i in v (including the commutators of weight 8 or more which do not appear explicitly above).

We now have the following lemmas.

Lemma 1 *Let K be a group satisfying properties* (1) *and* (2) *above, and suppose that the normal closure V of v in K has exponent* 7. *Suppose further that $(uw)^7 = u^7$ for all $w \in V$. Then $q_i(u,v)=1$ for $i=1,2,\ldots,6$.*

Lemma 2 *Let K be a group satisfying properties* (1) *and* (2) *above, and suppose that the normal closure V of v in K has exponent* 7. *Suppose further that $q_i(u,v)=1$ for $i=1,2,\ldots,6$, and that $q_i(uw_1,w_2)=1$ for $i=1,2,\ldots,6$ and for all $w_1 \in V$ and all $w_2 \in \gamma_3(K)$. Then $(uw)^7 = u^7$ for all $w \in V$.*

These were proved by straight-forward computer calculation. Using them we prove the following.

Lemma 3 *Let G be a* 2*-generator group of order 7^n and class at most* 29. *Let G have a power-commutator presentation with generators $a_1,a_2,\ldots,a_n$ (with $a_3=[a_2,a_1]$, $a_4=[a_2,a_1,a_1]$, $a_5=[a_2,a_1,a_2]$), where every generator has order* 7. *Let $k \geq 4$ and let $G_k = \langle a_k,a_{k+1},\ldots,a_n\rangle$. Then $q_i(u,v)=1$ $(1 \leq i \leq 6)$ for all $u \in G$ and all $v \in G_k$ if and only if $(uv)^7 = u^7$ for all $u \in G$ and all $v \in G_k$.*

Proof. The proof is by reverse induction on k, the result being trivial if $k=n+1$ since $G_{n+1}=\{1\}$.

First suppose that $(uv)^7=u^7$ for all $u \in G$ and all $v \in G_k$. Then taking $u=1$ we see that the normal subgroup G_k has exponent 7. So if $u \in G$ and $v \in G_k$ $(k \geq 4)$, then $K=\langle u,v\rangle$ satisfies the hypotheses of Lemma 1, and $q_i(u,v)=1$ for $i=1,2,\ldots,6$.

Next suppose that $q_i(u,v)=1$ for all $u \in G$ and all $v \in G_k$. We suppose by induction that $(uv)^7=u^7$ for all $u \in G$ and all $v \in G_{k+1}$. In particular this implies that $(a_k^i v)^7 = a_k^{7i} = 1$ for all $v \in G_{k+1}$, so that G_k has exponent 7. So if $u \in G$ and $v \in G_k$ $(k \geq 4)$, then $K=\langle u,v\rangle$ satisfies the hypotheses of Lemma 2, and $(uv)^7=u^7$. □

We are now in a position to prove a theorem which shows how the identities $q_i(u,v)=1$ can be used for exponent checking in groups of exponent 7.

Theorem 4 *Let G be a* 2*-generator group of order 7^n and class at most* 29. *Let G have a power-commutator presentation with generators $a_1,a_2,\ldots,a_n$ (with $a_3=[a_2,a_1]$, $a_4=[a_2,a_1,a_1]$, $a_5=[a_2,a_1,a_2]$), where every generator has order*

7. *Let S be the set of generators for representatives of the conjugacy classes of cyclic subgroups of G obtained using the Felsch-Neubüser algorithm as described above. Assume that*

(*i*) $(a_1a_2^i)^7 = 1$ *for* $i = 1, 2, \ldots, 6$;

(*ii*) $q_i(a_ra_s^\alpha \ldots a_t^\beta, a_q) = 1$ *for* $i = 1, 2, \ldots, 6$ *for all words* $a_ra_s^\alpha \ldots a_t^\beta a_q^\gamma \in S$ *with* a_q *of weight at least* 3.

Then G has exponent 7.

Proof. Clearly, factoring out by $[G^7, G]$ if necessary, we may assume that if $g \in G$, then g^7 lies in the centre of G. It follows that if g, h are conjugate in G then $g^7 = h^7$. We need to show that $x^7 = 1$ for all $x \in S$. Now the elements of S have one of the following forms: a_1v, $a_1a_2^iv$, a_2v, a_3v, v for some $v \in G_4 = \langle a_4, a_5, \ldots, a_n\rangle$. By hypothesis $a_1^7 = (a_1a_2^i)^7 = a_2^7 = a_3^7 = 1$. So it is sufficient to show that $(uv)^7 = u^7$ for all $u \in G$ and all $v \in G_4$.

We prove by reverse induction that if $k \geq 4$, then $(uv)^7 = u^7$ for all $u \in G$ and all $v \in G_k$. This is trivial for $k = n + 1$ since $G_{n+1} = \{1\}$.

Suppose by induction that $(uv)^7 = u^7$ for all $u \in G$ and all $v \in G_{k+1}$. Lemma 3 implies that $q_i(u, v) = 1$ $(1 \leq i \leq 6)$ for all $u \in G$ and all $v \in G_{k+1}$. We need to show that $(uv)^7 = u^7$ for all $u \in G$ and all $v \in G_k$.

Let $u \in G$ and $v \in G_k$. First note that, just as in the proof of Lemma 3, our inductive hypothesis implies that G_k has exponent 7, so we may suppose that $u \notin G_k$. There is an $x \in S$ such that u is conjugate to a power of x. Thus $u = x^{mg}$ for some $1 \leq m \leq 6$ and some $g \in G$. Let $x = a_1^{\alpha_1}a_2^{\alpha_2} \ldots a_n^{\alpha_n}$. If we let $y = a_1^{\alpha_1}a_2^{\alpha_2} \ldots a_{k-1}^{\alpha_{k-1}}$, then $x = ya_k^{\alpha_k}w$ for some $w \in G_{k+1}$. By induction, $x^7 = (ya_k^{\alpha_k})^7$, and we show that in fact $x^7 = y^7$. This is trivially true if $\alpha_k = 0$. But if $\alpha_k \neq 0$ then $ya_k^{\alpha_k} \in S$, and so our hypothesis implies that $q_i(y, a_k) = 1$ for $1 \leq i \leq 6$. As remarked above, our inductive hypothesis also implies that $q_i(u, v) = 1$ $(1 \leq i \leq 6)$ for all $u \in G$ and all $v \in G_{k+1}$. By Lemma 2 this implies that $(ya_k^{\alpha_k})^7 = y^7$. Hence

$$u^7 = x^{7mg} = (ya_k^{\alpha_k})^{7mg} = y^{7mg}.$$

Next consider $(uv)^7$. We can write $uv = (ya_k^\beta z)^{mg}$ for some $\beta \geq 0$ and some $z \in G_{k+1}$, and then

$$(uv)^7 = (ya_k^\beta z)^{7mg} = (ya_k^\beta)^{7mg}.$$

So to show that $(uv)^7 = u^7$ we need to show that $(ya_k^\beta)^7 = y^7$. Now, from the way that S was constructed, $y \in S$ and either $ya_k^\beta \in S$ or ya_k^β is conjugate to an element of the form yw with $w \in G_{k+1}$. If $ya_k^\beta \in S$ then $(ya_k^\beta)^7 = y^7$ by the argument just given above. If ya_k^β is conjugate to yw with $w \in G_{k+1}$, then $(ya_k^\beta)^7 = (yw)^7 = y^7$ by induction. Hence $(uv)^7 = u^7$. □

We use Higman's Lemma [5] to check that $q_i(a_r a_s^\alpha \dots a_t^\beta, a_q) = 1$ for $i = 1, 2, \dots, 6$ for all words $a_r a_s^\alpha \dots a_t^\beta a_q^\gamma \in S$ with a_q of weight at least 3. Its application to reduce exponent checking is described in Appendix B of [13]. In summary, it states that a p-group of class c has exponent p if every normal word of weight at most c has order dividing p. In particular, it implies that we only need to compute $q_i(a_r a_s^\alpha \dots a_t^\beta, a_q)$ for words $a_r a_s^\alpha \dots a_t^\beta a_q^\gamma$ of weight at most c, where c is the class of G.

When constructing the power-commutator presentation at each class for the increasing quotients of $R(2, 7)$, we only computed $q_i(a_r a_s^\alpha \dots a_t^\beta, a_q)$ for enough test words to reduce the order of the group to the order predicted by the Lie algebra calculations. We describe in Section 5 how we did this efficiently.

Finally, we obtained a consistent power-commutator presentation for a group G of order 7^{20416} and class 28. We now performed a complete exponent check on G. We checked that G admits an automorphism θ mapping a_1 to $a_1 a_2$ and mapping a_2 to a_1. If we let $G_2 = \langle a_2, a_3, \dots, a_{20416} \rangle$, then every element of G is the image of an element of G_2 under some power of the automorphism θ. To check that G has exponent 7, it is only necessary to check that G_2 has exponent 7. The proof of Theorem 4 shows that G_2 has exponent 7 provided all of the generators $a_2, a_3, \dots, a_{20416}$ have order 7 and $q_i(a_r a_s^\alpha \dots a_t^\beta, a_q) = 1$ for words $a_r a_s^\alpha \dots a_t^\beta a_q^\gamma \in S$ with $r \geq 2$. We tested these words using the reductions provided by Higman's Lemma.

5 The Baker-Campbell-Hausdorff formula

Let A be the free associative algebra with unity over the rationals $\mathbb{Q}$ that is freely generated by non-commuting indeterminates x, y. We extend A to the ring $\widehat{A}$ of formal power series consisting of the formal sums

$$\sum_{n=0}^{\infty} u_n,$$

where u_n is a homogeneous element of weight n in A. If $a \in \widehat{A}$, and if the homogeneous component of a of weight 0 is 0, then we define

$$\mathrm{e}^a = 1 + a + \frac{a^2}{2!} + \frac{a^3}{3!} + \dots$$

in the usual way. The product $\mathrm{e}^x \mathrm{e}^y \in \widehat{A}$ can be expressed in the form $1 + u$ for some $u \in \widehat{A}$, and

$$\mathrm{e}^x \mathrm{e}^y = \mathrm{e}^v$$

where

$$v = \sum_{n=1}^{\infty} (-1)^{n-1} \frac{u^n}{n}.$$

The Baker-Campbell-Hausdorff formula (see, for example, Jacobson [7, Chapter V]) enables us to compute the homogeneous components of v. The first few components are given below:

$$v = x + y - \frac{1}{2}[y,x] + \frac{1}{12}[y,x,x] - \frac{1}{12}[y,x,y] + \frac{1}{24}[y,x,x,y] + \dots.$$

One important (and surprising) feature of this expression is that the homogeneous components of v are all Lie elements of A (that is, elements in the Lie subalgebra of A generated by x and y with respect to the Lie product $[a,b] = ab - ba$). A similar formula holds for commutators:

$$[\mathrm{e}^y, \mathrm{e}^x] = \mathrm{e}^w,$$

where

$$w = [y,x] + \frac{1}{2}[y,x,x] + \frac{1}{2}[y,x,y] + \frac{1}{6}[y,x,x,x] + \frac{1}{4}[y,x,x,y] + \frac{1}{6}[y,x,y,y] + \dots.$$

These formulae sometimes allow us to define a group structure on a Lie algebra. One example is when L is a finite nilpotent Lie ring of order p^n and class at most $p-1$. We write the element v above as

$$v = v_1 + v_2 + \dots,$$

where v_i is a homogeneous Lie element of weight i, for $i = 1, 2, \dots$, and we consider the truncated expression

$$\widetilde{v}(x,y) = v_1 + v_2 + \dots + v_{p-1}.$$

The denominators of the coefficients that appear in $\widetilde{v}(x,y)$ are all coprime to p, and so if $a, b \in L$, then $\widetilde{v}(a,b)$ can be interpreted as an element of L. We define an operation "$\circ$" on L by setting

$$a \circ b = \widetilde{v}(a,b),$$

for $a, b \in L$. With this operation, $\langle L, \circ \rangle$ is a group of order p^n and class at most $p-1$, and every finite p-group of class at most $p-1$ arises in this way from a finite Lie ring. This appears as an exercise in Bourbaki [1, Chapter 2].

This connection breaks down for p-groups of class at least p, since the denominators of the coefficients of the terms of weight p in v are divisible by p. Nevertheless, we were able to construct part of the power-commutator presentation for $R(2,7)$ from that of $W(2,7)$ using the Baker-Campbell-Hausdorff formula.

We describe how this construction works at class 28; however we applied the same construction in computing the power-commutator presentation for the class c quotient of $R(2,7)$ for $23 \leq c \leq 28$. We assumed that the class 28 quotient of $L(2,7)$ is the class 28 quotient of $W(2,7)$. (There is a difficulty here, since at this stage we did not know that this was in fact the case; we will address this in Section 7.)

Let L be the class 28 quotient of $W(2,7)$, and let G be the class 28 quotient of $R(2,7)$. The Lie algebra calculations of [10] give a product presentation for L as a Lie algebra over $\mathbb{Z}_7$, with a basis $b_1, b_2, \ldots, b_{20416}$ and a set of relations

$$[b_i, b_j] = \sum_{k=i+1}^{20416} \beta_{(i,j,k)} b_k \ (1 \leq j < i \leq 20416).$$

For $i \geq 3$ the basis element b_i has a definition as a Lie product of b_1, b_2. Thus $b_3 = [b_2, b_1]$, $b_4 = [b_2, b_1, b_1]$ and so on. Each of the basis elements is assigned a weight, giving its degree as a Lie product of b_1, b_2, so that b_3 has weight 2, b_4 has weight 3, and so on. The Lie algebra L is graded; if b_i has weight u and b_j has weight v, then $[b_i, b_j]$ is a linear combination of basis elements of weight $u+v$. Thus $\beta_{(i,j,k)} = 0$ unless b_k has weight $u+v$. Similarly G has a power-commutator presentation with generators $a_1, a_2, \ldots, a_{20416}$, power relations $a_i^7 = 1$ $(1 \leq i \leq 20416)$, and commutator relations

$$[a_i, a_j] = a_{i+1}^{\alpha(i,j,i+1)} a_{i+2}^{\alpha(i,j,i+2)} \ldots a_{20416}^{\alpha(i,j,20416)}.$$

There is considerable choice in the matter, but it is possible to choose the generators of G and the basis elements of L so that their definitions exactly correspond to each other. In other words, if b_7 (for example) has definition

$$b_7 = [b_2, b_1, b_1, b_2]$$

as a Lie product of b_1 and b_2, then a_7 has definition

$$a_7 = [a_2, a_1, a_1, a_2]$$

as a commutator of a_1 and a_2. If we do this, then $\alpha_{(i,j,k)} = \beta_{(i,j,k)}$ whenever $\omega(a_k) = \omega(a_i) + \omega(a_j)$. Recall from Section 3 that $\alpha_{(i,j,k)} = 0$ whenever $\omega(a_k) < \omega(a_i) + \omega(a_j)$. As we noted above, $\beta_{(i,j,k)} = 0$ whenever $\omega(b_k) \neq \omega(b_i) + \omega(b_j)$. So the coefficients $\beta_{(i,j,k)}$ are determined by the coefficients $\alpha_{(i,j,k)}$. More critically, if $\omega(a_i) + \omega(a_j) \geq 23$ then all of the coefficients $\alpha_{(i,j,k)}$ are determined by the coefficients $\beta_{(i,j,k)}$.

Consider a basis element b_n of L where $\omega(b_n) \geq 23$. Then b_n has a definition of the form

$$b_n = [b_2, b_1, b_i, b_j, \ldots, b_k]$$

where $i, j, \ldots, k \in \{1, 2\}$. Let $c_1 = \mathrm{e}^x$ and $c_2 = \mathrm{e}^y$ and consider

$$c_n = [c_2, c_1, c_i, c_j, \ldots, c_k] = \mathrm{e}^{d_n(x,y)}$$

in $\widehat{A}$. The element $d_n(x,y)$ is an infinite $\mathbb{Q}$-linear combination of Lie elements of A of weight at least $\omega(b_n)$. We compute the truncated expression $\widetilde{d}_n(x,y)$

consisting of terms of weight at most 28. The denominators of the coefficients of the terms in $\widetilde{d}_n(x,y)$ are all coprime to 7, and so we can interpret $\widetilde{d}_n(b_1,b_2)$ as $\ell_n \in L$. It is easy to see that

$$\ell_n = b_n + \sum_{i=n+1}^{20416} \gamma_i b_i$$

for some coefficients γ_i, and we use the Baker-Campbell-Hausdorff formula to compute the values of these coefficients. Thus $\{\ell_n \,|\, \omega(b_n) \geq 23\}$ is a basis for L^{23}. Now suppose that $1 \leq j < i \leq 20416$ and that $\omega(b_i) + \omega(b_j) \geq 23$. Let b_i and b_j have definitions

$$b_i = [b_2, b_1, b_r, b_s, \ldots, b_t],\ b_j = [b_2, b_1, b_u, b_v, \ldots, b_w]$$

where $r, s, \ldots, t, u, v, \ldots, w \in \{1, 2\}$. Then

$$[[c_2, c_1, c_r, c_s, \ldots, c_t], [c_2, c_1, c_u, c_v, \ldots, c_w]] = \mathrm{e}^{d(x,y)}$$

in $\widehat{A}$. The element $d(x,y)$ is an infinite $\mathbb{Q}$-linear combination of Lie elements of A of weight at least $\omega(b_i) + \omega(b_j)$, and as above we compute the truncated expression $\widetilde{d}(x,y)$ consisting of terms of weight at most 28. Just as above, we can interpret $\widetilde{d}(b_1,b_2)$ as $\ell \in L$. It is easy to see that if $\omega(b_i) + \omega(b_j) = m$ then $\ell \in L^m$. If b_n is the first basis element of L of weight m, then we can write

$$\ell = \sum_{k=n}^{20416} \gamma_{(i,j,k)} \ell_k.$$

It turns out that $\alpha_{(i,j,k)} = \gamma_{(i,j,k)}$ for all $k \geq n$. So if $\omega(a_i) + \omega(a_j) \geq 23$, then the full commutator relation

$$[a_i, a_j] = a_{i+1}^{\alpha(i,j,i+1)} a_{i+2}^{\alpha(i,j,i+2)} \ldots a_{20416}^{\alpha(i,j,20416)}$$

can be computed from the product presentation for L using the Baker-Campbell-Hausdorff formula. Our proof of this fact relies on the assumption that L is the associated Lie ring of G. However, our claim that we have a power-commutator presentation for $R(2,7)$ does not rely on this proof, and so we omit it. We give a justification for relying on the results of this calculation in Section 7.

We use this observation as follows. Let us denote the class 27 and class 28 quotients of $R(2,7)$ by $R(2,7;27)$ and $R(2,7;28)$ respectively. Recall that the first step in constructing a power-commutator presentation for $R(2,7;28)$ is to construct one for the p-covering group of $R(2,7;27)$. To do this, we consider the relations

$$[a_i, a_j] = a_{i+1}^{\alpha(i,j,i+1)} a_{i+2}^{\alpha(i,j,i+2)} \ldots a_{20415}^{\alpha(i,j,20415)} \tag{3}$$

in $R(2,7;27)$ for $j = 1,2$. (The class 27 quotient has order 7^{20415}.) About half of these relations are definitions. For example, the relations $[a_2, a_1] = a_3$ and $[a_3, a_1] = a_4$ are the definitions of a_3 and a_4. We first introduce a new power-commutator presentation generator a_t for each of the relations which is *not* a definition, and substitute a modified relation

$$[a_i, a_j] = a_{i+1}^{\alpha(i,j,i+1)} a_{i+2}^{\alpha(i,j,i+2)} \dots a_{20415}^{\alpha(i,j,20415)} a_t, \tag{4}$$

with different values of the index t for each such modified relation. Then we add relations which make the new generators central and of order 7. The next step is to compute the new values of the commutators $[a_i, a_j]$ for $j > 2$. (These can always be deduced from the values of the commutators $[a_k, a_1]$ and $[a_k, a_2]$.) We now have a power-commutator presentation for a preimage of $R(2,7;28)$. (To obtain a presentation for the p-covering group of $R(2,7;27)$, we should also modify the power relations $a_i^7 = 1$ in a similar fashion, but our groups have exponent 7, and so this step is unnecessary.) This presentation may be inconsistent, and so we enforce consistency (see Appendix B of [13]), obtaining a consistent power-commutator presentation for our preimage of $R(2,7;28)$. The final step is to enforce exponent 7.

In our implementation, we only replaced relation (3) by relation (4) when $\omega(a_i) + \omega(a_j) < 23$. If $\omega(a_i) + \omega(a_j) \geq 23$, we replaced relation (3) by the relation computed from L with the Baker-Campbell-Hausdorff formula. The relations computed using this formula involve new power-commutator presentation generators of weight 28 corresponding to the basis elements of L of weight 28. In fact there is only one of these, a_{20416}, but the method would work equally well if there was more than one. This gave us a power-commutator presentation for a group which was intermediate between $R(2,7;28)$ and the p-covering group of $R(2,7;27)$. As usual, we then enforced consistency and exponent relations to obtain a consistent power-commutator presentation for $R(2,7;28)$. The advantage of this method is that at the final stage there are far fewer consistency and exponent relations which need to be enforced. Further, we were able to predict precisely which relations to enforce, because these were precisely the relations which had an effect in the computation of the class 22 quotient. This reduced the time for the final part of the calculation by a factor of at least two.

6 Resources

In Table 1 we summarise the ranks of the lower central factors of $R(2,7)$.

Class	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
Rank	2	1	2	3	6	9	12	23	36	61	94	159	260	406	640	985	1510
Total	2	3	5	8	14	23	35	58	94	155	249	408	668	1074	1714	2699	4209

Class	18	19	20	21	22	23	24	25	26	27	28
Rank	2157	2992	3795	4046	2850	240	96	14	14	2	1
Total	6366	9358	13153	17199	20049	20289	20385	20399	20413	20415	20416

Table 1: Ranks of central factors of $R(2,7)$

All calculations were carried out on a Sun UltraSPARC Enterprise 4000 server, having 3 GB of RAM. The process had maximum size 1.5 GB. In Table 2 we record the approximate CPU hours taken to construct the class k quotient of $R(2,7)$ for $1 \leq k \leq 28$.

Class	CPU hours
≤ 19	30
20	116
21	624
22	552
23	365
24	576
25	1219
26	624
27	960
28	1248

Table 2: Times in CPU hours for class constructions

The considerable variations in times taken to construct classes are primarily attributable to the use of new algorithmic techniques; for example, at class 22 we introduced more efficient formulae for exponent checking, the Baker-Campbell-Hausdorff formula was first used at class 23, and from class 26 onwards we only enforced consistency and exponent relations which were guaranteed to have an effect.

Let H be the 7-covering group of $R(2,7;28)$; it took 27 CPU hours to show using the general-purpose p-quotient algorithm that $H/H^7 = R(2,7;28)$, thus demonstrating that $R(2,7)$ has class 28.

The verification that the resulting power-commutator presentation on 20416 generators for the class 28 quotient is consistent took 190 CPU hours; it took 1221 hours to verify that the group has exponent 7.

Once the initial construction of a power-commutator presentation for a group is complete, it is sometimes possible to regenerate the presentation in a much shorter time than that taken by the original construction. This is largely because we can now avoid the redundant consistency and exponent checking performed by the general-purpose algorithm. No significant saving is possible here since the computations of power-commutator presentations at classes 26, 27 and 28 did not perform any redundant consistency or exponent checks. However, a small proportion of time could be saved through the use of the Baker-Campbell-Hausdorff formula at earlier classes.

7 Reliability of results

Since the construction of the power-commutator presentation for $R(2,7)$ required such significant resources, it is unlikely that the calculation will be reproduced in the near future.

When we reported on progress in constructing $R(2,7)$ at the "Group Theory and Computation" conference held in Sydney in December 1999, George Havas from the University of Queensland asked: "When you finish the calculation why should we believe the results?". Here we seek to provide a careful answer to this important question.

A first observation is that we can assert with a very high degree of confidence that we have a consistent power-commutator presentation for a 2-generator group of order 7^{20416}, class 28, and exponent 7. Although it required large resources and the use of special-purpose programs to construct this power-commutator presentation it is completely straight-forward (using the standard consistency algorithm) to verify that it is consistent. It is also relatively easy to verify that the group has exponent 7, although it would be difficult to do this without using commutator formulae such as the identities $q_i(u,v) = 1$ described in Section 4. The power-commutator presentation is also available for further testing, if required.

Next, note that the Lie algebra calculations of [10] imply that the class 28 quotient of $R(2,7)$ has order at most 7^{20416}. So, if our claim in the preceding paragraph is correct, we have a consistent power-commutator presentation for the class 28 quotient of $R(2,7)$.

We must justify our claim that $R(2,7)$ has class 28. The Lie algebra calculations imply that it has class at most 29. We had expected that the class of $R(2,7)$ would turn out to be 29, and consequently we verified that its class is 28 in three different ways.

Originally we used the Baker-Campbell-Hausdorff formula and a careful selection of test words to construct a consistent power-commutator presentation for a class 29 group G of order 7^{20418}. This group G is a descendant of the class 28 quotient. Our calculations implied that if $W(2,7)$ was the associated Lie ring of $R(2,7)$ then G was $R(2,7)$. However, when we performed a complete exponent check on G we found $g, h \in G$ whose 7-th powers generated $\gamma_{29}(G)$. So G could not be $R(2,7)$, and hence the associated Lie ring of $R(2,7)$ must be a proper quotient of $W(2,7)$. In other words, the associated Lie ring of $R(2,7)$ is $W(2,7)/I$ for some non-zero ideal I. Further, since the associated Lie ring of the class 28 quotient of $R(2,7)$ is the class 28 quotient of $W(2,7)$, it follows that $I \leq W(2,7)^{29}$. Finally, since $W(2,7)^{29}$ is irreducible as a module for the automorphism group of $W(2,7)$, this implies that $I = W(2,7)^{29}$, and hence that $R(2,7)$ has class 28.

We then did the calculation in a slightly different way. Once again we used the Baker-Campbell-Hausdorff formula to construct a power-commutator presentation for a group which was intermediate between the p-covering group for the class 28 quotient of $R(2,7)$ and the class 29 quotient. Then we systematically tested consistency and exponent, starting with the easiest test words first, until we found a small set of consistency and exponent checks which forced class 28. (We used the same set of consistency and exponent checks as in the earlier calculation, but we applied them in a different order.)

Finally we proved that $R(2,7)$ has class 28 using the general-purpose p-quotient algorithm (without using the Baker-Campbell-Hausdorff formula). We used the standard tails routine to build up a presentation for the p-covering group of $R(2,7;28)$ and applied consistency and exponent checks in the standard way. Once again, the calculation showed that $R(2,7)$ has class 28.

Using the general-purpose p-quotient algorithm, the following sets of consistency relations and identities equivalent to exponent verification are sufficient to force class 28. A sufficient set of consistency relations is $(a_i a_j)a_k = a_i(a_j a_k)$ with $i > j > k$, $k = 1,2$, $\omega(a_i) + \omega(a_j) \geq 22$. A sufficient set of identities is $[v,u,u,u,u,u,u] = 1$ where $u = a_1$, or a_2 or $a_1 a_2^i$ for $i = 1,2,3$, and where v is a power-commutator presentation generator of weight at least 17. These are particularly simple instances of the relation $q_1(u,v) = 1$ considered in Section 4. If G is a group of class at most 29 and if $u \in G$, $v \in \gamma_{17}(G)$, then

$$(uv)^7 = c \cdot [v,u,u,u,u,u,u]$$

where c is a product of 7-th powers. So it is a relatively easy calculation with an implementation of the general-purpose p-quotient algorithm to show that if H is the p-covering group of our group of class 28, then H/H^7 has class 28.

Our claim that we have a consistent power-commutator presentation for $R(2,7)$ relies to a large extent on Lie algebra calculations. But the Lie algebra calculations and the group calculations confirm each other. We calculated a power-commutator presentation for the class 22 quotient of $R(2,7)$ without using the Baker-Campbell-Hausdorff formula. Hence this calculation is independent of the Lie algebra calculations and shows that the order of the class 22 quotient coincides with the upper bound given by the Lie algebra calculations. The standard implementation of the general-purpose p-quotient algorithm was used to construct the class 18 quotient of $R(2,7)$; the order of each quotient obtained coincides with the orders obtained using both our modified group program and the Lie algebra calculations.

References

[1] N. Bourbaki, *Groupes et algèbres de Lie*, Hermann, Paris, 1972.

[2] V. Felsch and J. Neubüser, *An algorithm for the computation of conjugacy classes and centralizers in p-groups*, Lecture Notes Comput. Sci., 72, Springer-Verlag, Berlin, 1979, pp. 452–465.

[3] G. Havas and M.F. Newman, *Application of computers to questions like those of Burnside*, Lecture Notes Math., 806, Springer-Verlag, Berlin, 1980, pp. 211–230.

[4] G. Havas, G.E. Wall, and J.W. Wamsley, *The two generator restricted Burnside group of exponent five*, Bull. Austral. Math. Soc. **10** (1974), 459–470.

[5] G. Higman, *Some remarks on varieties of groups*, Quart. J. Math. Oxford Ser. (2) **10** (1959), 165–178.

[6] E.I. Khukhro, *On the adjoint Lie ring of the free 2-generator group of prime period and on Hughes's conjecture for 2-generator p-groups*, Mat. Sb. (N.S.) **118** (1982), 567–575.

[7] Nathan Jacobson, *Lie algebras*, Wiley-Interscience, New York, 1962.

[8] M.F. Newman, Werner Nickel and Alice C. Niemeyer, *Descriptions of groups of prime-power order*, J. Symbolic Comput. **25** (1998), 665–682.

[9] M.F. Newman and E.A. O'Brien, *Application of computers to questions like those of Burnside, II*, Internat. J. Algebra Comput. **6** (1996), 593–605.

[10] M.F. Newman and Michael Vaughan-Lee, *Some Lie rings associated with Burnside groups*, Electron. Res. Announc. Amer. Math. Soc. **4** (1998), 1–3.

[11] Charles C. Sims, *Computation with finitely presented groups*, Cambridge University Press, 1994.

[12] M.R. Vaughan-Lee, *Lie rings of groups of prime exponent*, J. Austral. Math. Soc. Ser. A **49** (1990), 386–398.

[13] Michael Vaughan-Lee, *The restricted Burnside problem*, second ed., Oxford University Press, 1993.

Department of Mathematics
University of Auckland
Auckland
New Zealand
obrien@math.auckland.ac.nz

Christ Church
University of Oxford
OX1 1DP
United Kingdom
michael.vaughan-lee@christ-church.oxford.ac.uk

Last revised July 2001